May 2021

Active Differential Privacy Budget Management

N/A

Active Differential Privacy Budget Management

Background

Datasets and data derived therefrom may include and/or reveal information regarding one or more individuals whose records are contained in the dataset. For example, a dataset from a medical study may include an age of an individual who participated in the medical study. Oftentimes, such data and/or the release thereof is the subject of privacy concerns. For example, data from a dataset may be combined with other data (e.g., publically available data, etc.) to reveal the identity of individuals whose records are contained in the dataset. This is generally undesirable. Therefore, removing personally identifiable information (PII) such as names, Social Security numbers, and the like from a dataset is often not enough to ensure that the dataset does not reveal information regarding individuals whose records are contained in the dataset and/or preventing data from the dataset from being linked back to such individuals. For example, in the 1990's it was shown that "anonymized" records (e.g., records with direct identifiers such as names, etc. removed) summarizing information about hospital visits could be directly linked to their subject by cross-correlating the anonymized records with voter registration data. This is generally referred to as privacy leakage. It is worth noting that privacy leakage can still occur where primary data (e.g., an element directly contained in a dataset, etc.) is not released. In many scenarios, the release of results produced by analyzing a dataset (e.g., statistical measures such as mean, median, standard deviation, etc.) may similarly cause privacy leakage. Indeed, an individual need not be included in a dataset for the release of results produced by analyzing the dataset to cause privacy leakage of information regarding the individual. For example, an insurance provider may learn of a study on heart disease indicating that, of those sampled, individuals with brown hair had a significant increase in heart attacks, and may know that client Fred has brown hair (and therefore an increased risk of heart attack based on the study), and may increase Fred's insurance premium as a result.

To solve this challenge and facilitate the release of data without violating individuals' privacy, systems and methods of differential privacy were developed. Differential privacy facilitates the quantification of privacy leakage and provides formal privacy guarantees regarding the release of data such as datasets. However, often differential privacy guarantees (e.g., quantifying an amount of privacy leakage associated with a release of data, etc.) must be

developed on a case-by-case basis. For example, the amount of privacy leakage associated with a release of information may depend on the type of analysis used to generate the information being released. Moreover, each release of information may incur additional privacy leakage. For example, if many different information releases occur, the total privacy leakage may grow even though the privacy leakage of each individual release is limited. Policy makers often want to limit the total privacy leakage, which requires composing the individual privacy leakage of each release. Therefore, it is often necessary to review these factors manually to develop an accurate model of privacy leakage and/or determine countermeasures to ensure adequate privacy (e.g., adding random noise to the information released, etc.).

However, in many scenarios it may be unrealistic to manually review every release of information (e.g., manually compose the privacy leakage from every release of information, etc.) to ensure differential privacy. For example, in the online-retail environment, retailers may request daily summaries from advertisement-serving platforms regarding the effectiveness of their ad-campaigns. For an ad-serving platform having thousands or hundreds of thousands of customers, manually reviewing each request to determine if it would exceed the desired total privacy leakage may be infeasible. Therefore, there is a need for systems and methods that facilitate programmatic access (e.g., those that limit an amount of manual review required, etc.) to datasets and/or data derived therefrom (e.g., statistical measures, etc.). Described herein is a platform for providing access to datasets and/or data derived therefrom while maintaining differential privacy (e.g., quantifying privacy leakage and/or limiting total privacy leakage, etc.). Moreover, a number of usability features to improve the ease of user interaction with the platform are discussed.

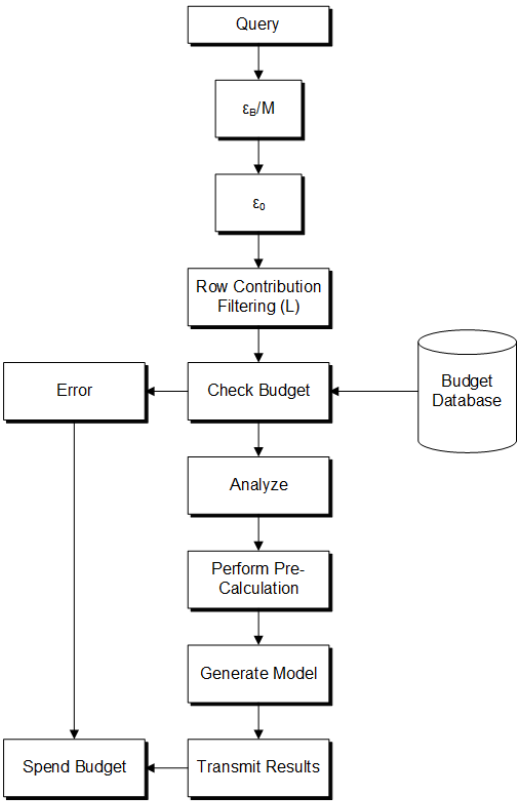

FIG. 1

Overview

Referring now to FIG. 1, a method of processing a user query for data is shown. ε_B may

refer to a privacy budget. In various embodiments, ε_B is specific to one or more factors. For example, ε_B may be a privacy budget for a specific customer for a specific data-day. Data-days are discussed in greater detail below. ε_B may be a static variable (e.g., every customer has the same privacy budget, etc.) or may be a dynamic factor (e.g., some customers are given different privacy budgets, etc.). In various embodiments, ε_B is a real number. For example, ε_B may be equal to 1.78. M may be a model limit. For example, M may be a limit of a model per customer per data-day. In some embodiments, M is equal to 100. However, other values are possible. ε_0 may be an overall query privacy budget. In various embodiments, $\varepsilon_0 = \varepsilon_B/M$. L may be a user-specified input-filtering 2-norm limit. In various embodiments, the method includes one or more pre-calculation operations. ε_N is a noise privacy budget. In various embodiments, ε_N is equal to $ln(1+(e^{\varepsilon 0}-1)/p)=f_N(p, \varepsilon_0)$, where p is a user-specified sampling ratio (e.g., to discard rows, etc.).

Referring generally to FIG. 1, the method may include receiving a query such as a query for statistical measures (e.g., mean, median, standard deviation, variance, etc.) associated with a dataset such as a dataset describing user engagement with online content (e.g., online ads, etc.). For example, a database may include records describing a number of online interactions with content items and identifiers (e.g., device identifiers, etc.) associated with the number of online interactions and an individual may query the database to retrieve information associated with the number of online interactions (e.g., aggregate volume of interactions, interactions by device type, etc.). In various embodiments, the query is received from an external computing system such as a computing system associated with a retailer.

In various embodiments, the method includes calculating an overall query privacy budget ε_0. In various embodiments, ε_0 is equal to ε_B/M. In some embodiments, the method includes one or more usability features, discussed in detail below, which may affect the value of ε_0. In various embodiments, the method includes determining L. In various embodiments, row contribution filtering facilitates preventing users from skewing outputs. For example, row contribution filtering may prevent users from injecting a single row having a large value for inputs, thereby skewing the outputs. In some embodiments, L is determined based on a default limit (e.g., an upper and/or lower bound, etc.). For example, the default limit may vary dynamically based on various factors (e.g., by customer, by user, by query type, etc.). Additionally or alternatively, L

may be determined based on a hard limit (e.g., an upper and/or lower bound, etc.). In various embodiments, row contribution filtering requires users to pre-commit to a maximum row size.

In various embodiments, the method includes comparing a privacy budget associated with the query to an allowed (e.g., remaining, etc.) privacy budget associated with the user/customer. For example, a particular query may relate to information spanning a number of data-days and comparing the privacy budget associated with the query to the allowed privacy budget may include checking the privacy budget for each data-day in the query with the remaining privacy budget for each data-day (e.g., using budget database, etc.). If there is sufficient remaining privacy budget to enable the query, the method may proceed to analyze the dataset based on the query. Alternatively, if there is insufficient remaining privacy budget to enable the query (e.g., the query is over budget, etc.), the method may include transmitting an error (e.g., describing that the query is over budget, etc.). In some embodiments, transmitting the error includes spending an amount of privacy budget (e.g., due to the release of information associated with the error, etc.).

In various embodiments, the method includes performing one or more pre-calculations (as described above). For example, the method may include determining a user count associated with the query to determine whether the query relates to a sufficient number of users (e.g., isn't producing granular data on a single user/device, etc.). For example, the method may include determining the user count associated with the query and comparing the determined user count to a threshold. If the query relates to an insufficient number of users (e.g., too few users, the determined user count is less than the threshold, etc.) the method may include transmitting an error. In some embodiments, transmitting the error includes spending an amount of privacy budget (e.g., due to the release of information associated with the error, etc.). If the query relates to a sufficient number of users, the method may proceed to generate a model associated with the query. For example, the method may include generating a linear regression model of the form $y=mx+b$ describing conversion information associated with a number of online interactions. In various embodiments, the method includes transmitting results associated with the model and/or the query such as a slope and/or a y-intercept associated with the model (e.g., m and/or b in the example above, etc.). In various embodiments, the results are transmitted to an entity that submitted the query. In various embodiments, the method includes spending a privacy budget

associated with the query. For example, the method may include updating a budget database to reflect the privacy budget used for each data-day associated with the query and/or transmitted results.

In various embodiments, the method described above may be implemented using one or more computing systems. For example, the method may be implemented using a distributed processing system having one or more processing circuits, each including one or more processors and one or more memories, the memories having instructions stored thereon that, when executed by the one or more processors, cause the one or more processing circuits to perform the various operations described herein.

Discussion of Factors Affecting Privacy Budgets and/or Usability

Before turning to various possible augmentations of the method/system described above, various factors affecting privacy budgets and/or usability are discussed.

Budgets

In various embodiments, customers may share a privacy budget. For example, a number of customers that routinely request information derived from a data source may all share a privacy budget. Additionally or alternatively, customers may receive their own budget. In various embodiments, information is organized into datasets. For example, device interaction data may be organized into a dataset according to a source of the data. In various embodiments, each dataset receives its own budget.

Over Budget: What Happens?

In various embodiments, the method described above may transmit an error in response to determining that a query violates (e.g., exceeds, etc.) an amount of allotted/remaining privacy budget. In some embodiments, transmitting the error includes transmitting an error without supplemental information (e.g., information describing a cause of the error, etc.). In some embodiments, transmitting the error includes transmitting an error with supplemental information. For example, the error may include information describing which day(s) exceeded the privacy budget and/or that a specific user has exceeded their allotted budget (e.g., a customer has remaining budget but an individual associated with the customer that is making the query has

exhausted their portion of the customer budget, etc.). Additionally or alternatively, the method may include removing data-days that have exhausted budgets from the query and re-running the query. For example, the method may include identifying one or more data-days included in the original query that have exhausted budgets and generating an augmented query based on the original query by removing the one or more data-days from the original query. In various embodiments, each error-handling method is associated with an amount of privacy budget spend. For example, a first error including a large amount of supplemental information may be associated with a larger expenditure of privacy budget than a second error including no supplemental information.

Determining a User Count

As described above, the method may include one or more pre-calculations such as determining a user count. In various embodiments, determining the user count includes determining a noisy user count (e.g., a count of user associated with a query with random noise

added to the count, etc.). In some embodiments, the user count is calculated using partition selection as described in *"Differentially private partition selection" (Desfonaines et al., 2020)*.

Usability Features

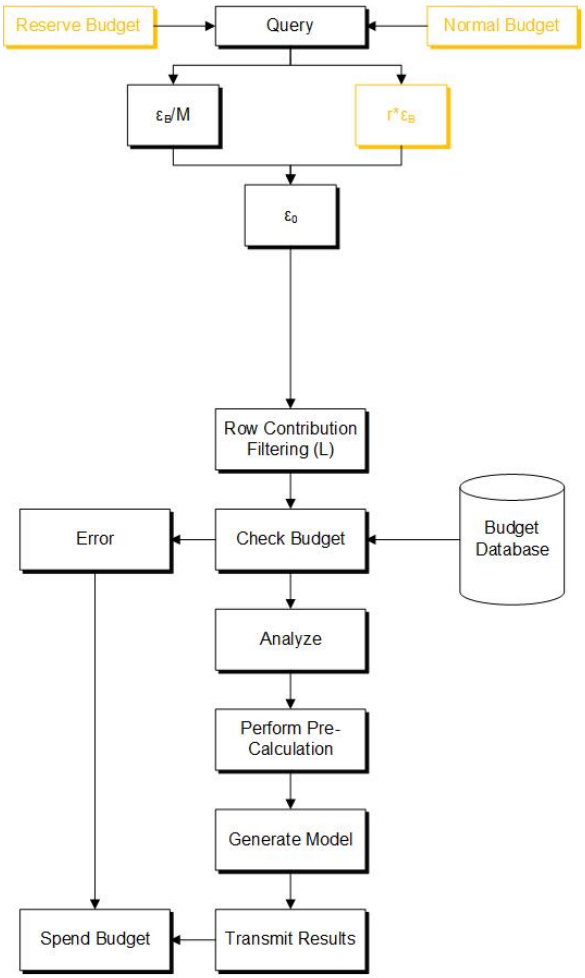

FIG. 2

Referring now to FIG. 2, another method of processing a user query for data is shown. In various embodiments, the method of FIG. 2 is similar to the method of FIG. 1 with added usability features. In various embodiments, *r* is a user-specified privacy ratio per query. For example, *r* may allow users to generate queries having more noise, thereby conserving a greater amount of privacy budget per query. In some embodiments, *r* is equal to *1/M*. In various embodiments, the privacy budget ε_B may comprise a normal portion and a reserve portion. For example, ε_B may include a reserve portion that may be activated by a system administrator (e.g., of a system implementing the method of FIG. 2, etc.). In various embodiments, the reserve portion may be used in emergency situations where the normal budget is inadvertently consumed (e.g., through an incorrectly parameterized query, via an inexperienced user, etc.). In some embodiments, a whitelist including users that may access the reserve portion may be maintained to determine access to the reserve portion. In various embodiments, calculating $r*\varepsilon_B$ improves usability of the method/system for users. For example, a user may select a value of *r*, thereby enabling a larger number of higher-noise queries than otherwise possible. In some embodiments, user selection of *r* is only available to a select number of users specified by a whitelist. In various embodiments, these features may facilitate preventing a single individual (e.g., an inexperienced junior data scientist, etc.) from inadvertently spending an entire customer's privacy budget allocation on a

single query (e.g., an incorrectly parameterized query, an overbroad query, etc.). In some embodiments, the number of queries per user and/or per customer are limited (e.g., user can only make 5 queries a day, etc.).

In various embodiments, the method facilitates sandbox models. For example, the method may enable users to test out query parameters on a fake dataset (e.g., a generated dataset that does not include real online interaction data, etc.). In this way, users may determine query parameters through trial-and-error without spending on privacy budgets.

In various embodiments, the method of FIG. 2 may be implemented using one or more computing systems. For example, the method may be implemented using a distributed processing system having one or more processing circuits, each including one or more processors and one or more memories, the memories having instructions stored thereon that, when executed by the one or more processors, cause the one or more processing circuits to perform the various operations described herein.

In various embodiments, the methods/systems described here may facilitate the methodical release of information in a differentially private manner by tracking access characteristics associated with datasets (e.g., which datasets were accessed and what information was accessed from those datasets, etc.).

Abstract

A data processing system may facilitate the methodical release of information in a differentially private manner by tracking access characteristics associated with datasets. The data processing system may maintain a privacy budget allocation for entities and/or users and may calculate privacy budget expenditures based on queries submitted by the entities and/or users. The data processing system may process entity and/or user queries for information from one or more datasets and may track privacy budget expenditures in relation to privacy budget allocations.